(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 December 2003 (24.12.2003)

PCT

(10) International Publication Number
WO 03/107256 A1

(51) International Patent Classification[7]: G06K 7/00. G01S 13/02, G07C 9/00, G06K 19/07

(21) International Application Number: PCT/GB03/02532

(22) International Filing Date: 12 June 2003 (12.06.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0213724.8 14 June 2002 (14.06.2002) GB

(71) Applicant *(for all designated States except US)*: **BTG INTERNATIONAL LIMITED** [GB/GB]; 10 Fleet Place, Limeburner Place, London EC4M 7SB (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **DAVIDSON, William, E.** [CA/US]; 3530 Hamstead Court, Durham, NC 27707 (US). **TURNER, Christopher, Gordon, Gervase** [GB/GB]; 53 Brill Road, Oakley HP18 9QN (GB).

(74) Agent: **BINGHAM, Ian, Mark**; BTD International Limited, 10 Fleet Place, Limeburner Lane, London EC4M 7SB (GB).

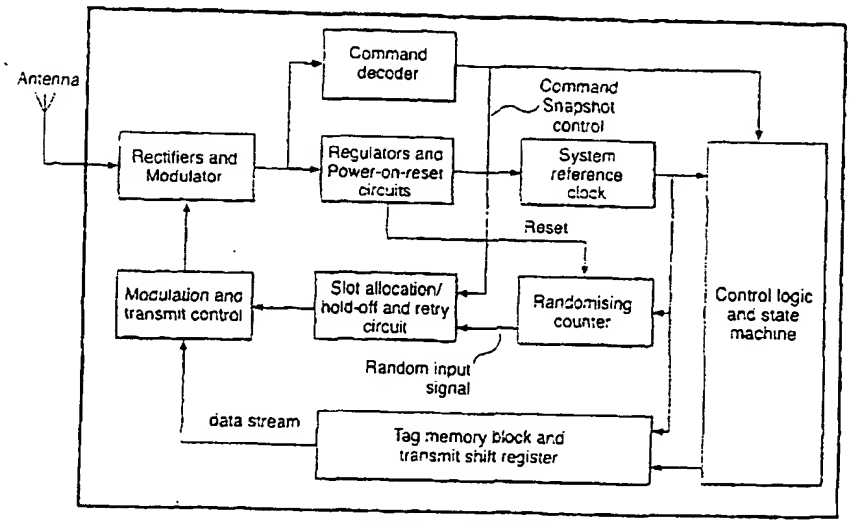
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ELECTRONIC IDENTIFICATION SYSTEM



RFID Chip - Block Diagram

(57) Abstract: The invention relates to a method of identifying a plurality of transponders each of which transmits data at intervals to a receiver. The invention also relates to an identification system comprising a plurality of transponders and a receiver, to the transponders themselves and to an integrated circuit for use in a transponder. The transponder repeats data to the receiver at random or pseudo-random intervals in length. The intervals are directly or indirectly dependent on the output signal from a counter responsive to a physical characteristic of the transponder.

WO 03/107256 A1

ELECTRONIC IDENTIFICATION SYSTEM

FIELD OF INVENTION

This invention relates to a method of identifying a plurality of transponders each of which transmits data at intervals to a receiver. The invention also relates to an identification system comprising a plurality of transponders and a receiver, to the transponders themselves and to an integrated circuit for use in a transponder.

BACKGROUND TO THE INVENTION

Identification systems are known in which a plurality of transmitters, typically transponders (commonly called tags), are activated by a power signal (or an "interrogation signal") and then transmit signals, usually containing identification data to a receiver, which typically forms part of the interrogator. The signals may be transmitted in many ways, including electromagnetic energy, eg. radio frequency (RF), infra red (IR), coherent light and sound, eg. ultra-sound. For example the transmission may be achieved by actual emission of RF energy by the transponders, or by the modulation of the reflectivity of an antenna of the transponder, resulting in varying amounts of RF energy in the interrogation signal being reflected or back-scattered from the transponder antenna.

Radio Frequency Identification systems are used to remotely identify, take a census of, locate or otherwise interact with people, objects or groups or clusters of people or objects. The systems usually comprise interrogators also known as readers, and transponders also known as tags.

It is not usually a problem for a reader to communicate with a single tag which is presented to the reader, such as in an access control system. However in the situation where many tags may be present in a reader's field of views, such as a crowd of people, or a pallet load of goods having tags attached, the transmissions by the tags would occur together and cause collisions, rendering the transmissions unusable due to mutual interference. A number of arbitration methods have been developed to enable a reader to sort and/or isolate and transact with these large

populations of tags. These methods are known variously as anti-collision schemes or collision-arbitration algorithms.

In one example described in US 5,537,105 (corresponding to EP 494114 B1) by Marsh et al, the whole contents of which are incorporated herein, the transponders on receipt of an interrogation signal repeatedly transmit a response signal containing data which identifies the transponder. The interrogator detects successful identification of any transponder and briefly modifies the interrogation signal to indicate the successful identification. Each transponder includes a logic circuit responsive to a respective modification in the interrogation signal to cease transmission of its own response signal. The response signals are transmitted at random intervals until the identity of a transponder is successfully read and acknowledged by the reader and placed into a dormant or gagged state. US5699066 (corresponding to EP0585132) and PCT application GB98/01385 (corresponding to WO/985142) also describe methods in which the response signals are transmitted at pseudo-random intervals. The whole contents of EP0585132 and WO/985142 are incorporated herein by reference.

Other examples of such methods are described in US5699096, Cole WO 01/41043 A1, and Maletsky US6104279.

Methods have been used to improve the randomness of the response intervals. In EP 467036 B1, the whole contents of which are herein incorporated, the identification system uses a pseudo-random delay between transponder data transmissions. In this example, a linear recursive sequence generator is seeded by the transponder identification address to provide the pseudo-random delay between tag data transmissions. US5550547 describes a similar system in which the tag sends out a 64 bit ID code at intervals determined by a random number generator. US6104279 describes a system in which remote units re-transmit their bit pattern at random intervals. It further mentions that there are many techniques to produce a random number; for example the identification number can provide the seed for a random number generator permitting the user to individually seed each tag with a different random number.

Another method is based on slotted polling or slotted Aloha schemes in which tags randomly select a time slot in which to transmit and then transmit when it is their turn to do so. The theory is that because slots are randomly selected, sooner or later all tags will have had the opportunity to transmit messages 'in the clear'. WO 01/41043 describes such a system in which RFID tags randomly select a slot in which to transmit. In a practical implementation the slot selection by a tag is made on a pseudo-random basis, using a seed for a random number generator, which is derived from either part of the data held on the tag or by pre-programming a seed where the tag is manufactured. The possibility is great that many tags will have the same slot allocation choice. The fewer the number of slots to choose from, the greater will be the probability that many tags will 'randomly' select the same slot time and so will always collide and will therefore never be successfully read.

All the systems described rely on the use of random or pseudo-random timing of the tag transmission or reply signal. The random number generators (RNG) or pseudo-random number generators (PRNG) referred to in all the specifications above, rely on a recursive method of generating a random number from a seed. Because of their nature, seeded random number generators will always repeat the randomisation pattern and the pattern will be fully predictable. If the recursive random number generator had an infinite length, each seed would result in a unique pattern. However, RNG's have a finite length and in real applications will be typically 10 to 16 bits long. It is probable that in a cluster of 100 tags there will be several tags that will have a similar or identical transmit repeat [slot] pattern. If these tags were placed in the reader field at the same time, they would repeatedly transmit their identity together and hence would always clash and would never be successfully read. The problem is that seeded random number generators are not truly random (hence they are known as pseudo-random) and therefore do not provide the level of protection against clashes that is required for the efficient operation of the collision arbitration systems described in the cited patents.

In PRNG systems – the random pattern is only random for different seed values. The same seed value produces a predictable and consistent pattern. The finite length of an RNG will result in many tags having exactly the same repeat pattern. Furthermore, no matter how long the seed, only a subset of the seed will actually

influence the pattern. The shorter the RNG shift register, the smaller the number of different random numbers or patterns.

Summary of the invention

The present invention strives to overcome the disadvantages in the prior art and eliminate the aforesaid disadvantage of a pseudo-random slot selection or random transmit hold-off method.

The method of the present invention also strives to overcome the inherent problem of generating a random slot number or transmit hold off delay in RFID tags – when using a seeded random number generator. A seeded RNG is by its nature only pseudo-random in that for a given register length and tapped feedback points, a seed of a given value will always yield the same pattern.

In one aspect of the present invention there is provided an identification system comprising a reader including a transmitter for transmitting a signal and a plurality of transponders, each transponder including a receiver for receiving the reader signal and a transmitter for generating a response signal containing data which identifies the transponder, the transponder being adapted to repeat the transmission of the response signal at intervals which are random or pseudo-random in length, characterised by a circuit responsive to a physical characteristic of the transponder, the intervals between the response signals being directly or indirectly dependent on the output signal from said circuit.

The physical characteristic of the circuit, in a preferred embodiment part of an RFID chip, provides a "true random result", the output signal from the circuit affecting the randomness of the intervals between the response signals.

In a preferred embodiment said circuit comprises a counter driven by a clock, which may or may not be the same clock which used to drive the logic of the chip, the output from the counter providing a random number, or a random interval signal or providing a seed value for a random number generator. The counter and the clock may be reset upon activation of a POWER-ON-RESET (POR) circuit.

In another aspect of the invention there is provided a method of identifying a plurality of transponders comprising; exposing a transponder to RF whereby a capacitor is charged to a predetermined value to activate a POWER-ON-RESET (POR) circuit, the transponder being responsive to a command signal from a reader to repeat the transmission of a response signal, containing data which identifies the transponder, at intervals which are random or pseudo-random in length, characterised by a circuit responsive to activation of the POR to provide an output signal when the command signal has been received, the output signal providing a random number or a seed for a random number generator used to determine a slot selection or random transmit repeat (hold-off) value for the response signals.

In a further aspect of the invention there is provided a transponder comprising receiver means for receiving a reader signal, transmission means for transmitting a response signal containing data which identifies the transponder, the transponder being adapted to repeat the transmission of the response signal at intervals which are random or pseudo-random in length, characterised by a circuit responsive to a physical characteristic of the transponder, the intervals between the response signals being directly or indirectly dependent on the output signal from said circuit.

In a further aspect of the invention there is provided an integrated circuit for use in a transponder, comprising receiver means for receiving a reader signal, transmission means for transmitting a response signal containing data which identifies the transponder, the integrated circuit being adapted to repeat the transmission of the response signal at intervals which are random or pseudo-random in length, characterised by a random circuit responsive to a physical characteristic of the transponder, the intervals between the response signals being directly or indirectly dependent on the output signal from said circuit. In a preferred embodiment the integrated circuit is a RFID chip.

Description

The invention will be described further by way of example with reference to the accompanying drawing, in which:

Figure 1 is a block diagram showing a circuit for use in a transponder according to a first embodiment of the invention and

Figure 2 shows a timing diagram illustrating the operation of four transponders of the present invention.

Figure 3 shows a block diagram of a typical RFID chip incorporating the circuit according to the first embodiment of the invention.

A transponder (tag) comprises an integrated circuit in the form of an RFID chip a part of which is shown in Figure 1. When the RFID chip is exposed to an RF field or when voltage is applied – the chip goes through a POWER-ON-RESET (POR) sequence. When the recovered DC supply voltage is stable, the POR circuit provides a signal to the circuits on the chip, which signal initialises or resets the chips circuits. At this point the clock starts running and drives the counter. The output of the counter is routed to the circuits in the chip that require a random number. Examples of these circuits could be the slot selection described in WO 01/41043, or the random transmit timer described in US5699096 or US6104279. It could also for example be used to derive the tag signature described in the international committee draft standard CD ISO 18000-6 type A or the signature described in EP1001366A2

The instant, that POR occurs with respect to the application of RF power, can vary substantially from chip to chip or from one power on sequence to the next, due to many factors. One of these factors is the delay due to the time it takes for the DC power storage capacitor to charge. Only when the capacitor has charged to a predetermined value will the POR circuit activate. This charging time is determined by a number of mechanisms:-

1. The RF voltage applied to the chip
2. The impedance of the antenna – in particular the series resistance – often called the Radiation Resistance
3. The size of the DC (VDD) storage capacitor
4. The actual POR voltage threshold

5. The leakage resistance in the circuit
6. The impedance of the rectifier diodes

Referring to the timing diagram in Figure 2, at some point in time after the RF has been applied to the chip, a reader will issue a command which is received by all chips within range. It is probable that all chips within range will have started their clocks running at slightly different times due to the charge times of their DC storage capacitor and due to the slightly different POR characteristics between tags.

When the chips receive the command (which could be a wake-up or other command etc) the value in the counter in each of the chips will be different due to the slightly different start times. The value at the instant of the command (command snapshot) is used as the random number or as a seed for a random number generator used to determine the slot selection or random transmit repeat (hold-off) value. Therefore each chip will have a different value to be used for slot allocation or transmit hold-off time.

Furthermore if the counter in each and every chip continues to run and because no two counters will have the same clock period due to physical variances etc – the value in one chip's counter will be different (appear to be randomly different) with respect to the value in all other chips at any point in time. The clock frequency of each chip clock will be slightly different due to supply voltage variations, chip manufacturing variations, chip leakage etc. Therefore each time a command is received from a reader (causing a command snapshot) each chip will have a different value in their counter with respect to other chips and therefore the value that is used to allocate a transmit slot or hold off delay will be different for each chip and will be truly random.

It will be appreciated that the method described does not dictate the use of a random number generator – but that the snapshot value of the free running counter could be used directly to allocate a slot in which the tag will transmit, or alternatively the value could be used to seed a RNG. It will also be appreciated that the method disclosed could also be used (this is the preferred embodiment) to randomly assign a transmit hold-off period which need not conform to any slotting mechanism but

which provides true randomisation of tag data transmissions. As the tag population increases, so does the total time it takes to read a population of tags. This is beneficial using this method, because the longer the free running counter continues to run, the more the count value will diverge from the counters in all other tags due to the natural variation in clock frequencies due to chip manufacturer process, temperature, varying RF fields etc.

It will be further appreciated that the method taught, is not only applicable to the randomisation of tag transmissions in RFID systems but this method may also be used to provide any random number that may be required in a tag circuit such as a session identity or tag signature etc.

Figure 3 shows the integration of the invention into an RFID chip. In the chip, the slot allocation circuit which could also be a transmit hold-off and retry circuit, is driven by two control signals. A first control signal is a random input signal derived from the system clock and the randomising counter. A second control signal, called the command snapshot control, causes the slot allocation circuit to take a snapshot of the random input signal value, and uses this value to allocate a slot in which the tag will transmit alternatively will use this value as a hold-off delay value for the next transmission by the tag. Each time the tag receives a command, which may or may not necessarily be directed to the tag itself, the command decoder generates a snapshot signal, thereby causing a fresh slot to be randomly selected or hold-off value to be randomly generated. It will therefore be evident to those skilled in the art, that the randomness of the method is entirely dependent on physical characteristics which will be different from every other RFID chip or tag.

It will be seen that the invention efficiently attains the objects set forth above, among those made apparent from the preceding description. Since certain changes may be made in the above embodiments without departing from the scope of the invention, it is intended that all matter contained in the above description or shown in the accompanying drawings be interpreted as illustrative and not in a limiting sense.

CLAIMS

1. An identification system comprising a reader including a transmitter for transmitting a signal and a plurality of transponders, each transponder including a receiver for receiving the reader signal and a transmitter for generating a response signal containing data which identifies the transponder, the transponder being adapted to repeat the transmission of the response signal at intervals which are random or pseudo-random in length, characterised by a counter driven by a clock, the output from the counter providing a random number or providing a seed value for a random number generator to affect the randomness of the intervals between the response signals.

2. An identification system as claimed in claim 1, wherein the counter and the clock are reset upon activation of a POWER-ON-RESET (POR) circuit.

3. An identification system as claimed in claim 1 or claim 2, wherein the counter and clock is part of an RFID chip.

4. A transponder comprising receiver means for receiving a reader signal, transmission means for transmitting a response signal containing data which identifies the transponder, the transponder being adapted to repeat the transmission of the response signal at intervals which are random or pseudo-random in length, characterised by a counter driven by a clock, the output from the counter providing a random number or providing a seed value for a random number generator to affect the randomness of the intervals between the response signals.

5. A transponder as claimed in claim 4, wherein the counter and the clock are reset upon activation of a POWER-ON-RESET (POR) circuit

6 An integrated circuit for use in a transponder, comprising receiver means for receiving a reader signal, transmission means for transmitting a response

signal containing data which identifies the transponder, the integrated circuit being adapted to repeat the transmission of the response signal at intervals which are random or pseudo-random in length, characterised by a counter driven by a clock, the output from the counter providing a random number or providing a seed value for a random number generator to affect the randomness of the intervals between the response signals.

7 An integrated circuit as claimed in claim 6, wherein the counter and the clock are reset upon activation of a POWER-ON-RESET (POR) circuit.

8 An integrated circuit as claimed in claim 7 or claim 8, wherein the integrated circuit is part of an RFID chip.

9 A method of identifying a plurality of transponders, comprising exposing a transponder to RF whereby a capacitor is charged to a predetermined value to activate a POWER-ON-RESET (POR) circuit, the transponder being responsive to a command signal from a reader to cause or repeat the transmission of a response signal, containing data which identifies the transponder, at intervals which are random or pseudo-random in length, characterised by a counter driven by a clock responsive to activation of the POR to provide an output signal when the command signal has been received, the output signal providing a random number or a seed for a random number generator, a slot selection or random transmit repeat (hold-off) value for the response signals being dependent directly or indirectly on said output signal.

10 An identification system as claimed in claim 1 or claim 2, wherein the counter and clock are routed to a latch such that when a command is received by the transponder, the instantaneous value of the counter is stored in the latch.

11 An identification system as claimed in claim 10, wherein the latch provides a random number or a seed value for a random number generator to affect the randomness of the intervals between the response signals.

12 A transponder as claimed in claims 4 or 5, wherein the counter and clock are routed to a latch such that when a command is received by the transponder, the instantaneous value of the counter is stored in the latch.

13. A transponder as claimed in claim 12, wherein the latch provides a random number or a seed value for a random number generator to affect the randomness of the intervals between the response signals.

14 An integrated circuit as claimed in claim 6 or 7, wherein the counter and clock are routed to a latch such that when a command is received by the transponder, the instantaneous value of the counter is stored in the latch.

15 An integrated circuit as claimed in claim 14, wherein the latch provides a random number or a seed value for a random number generator to affect the randomness of the intervals between the response signals.

Fig.1

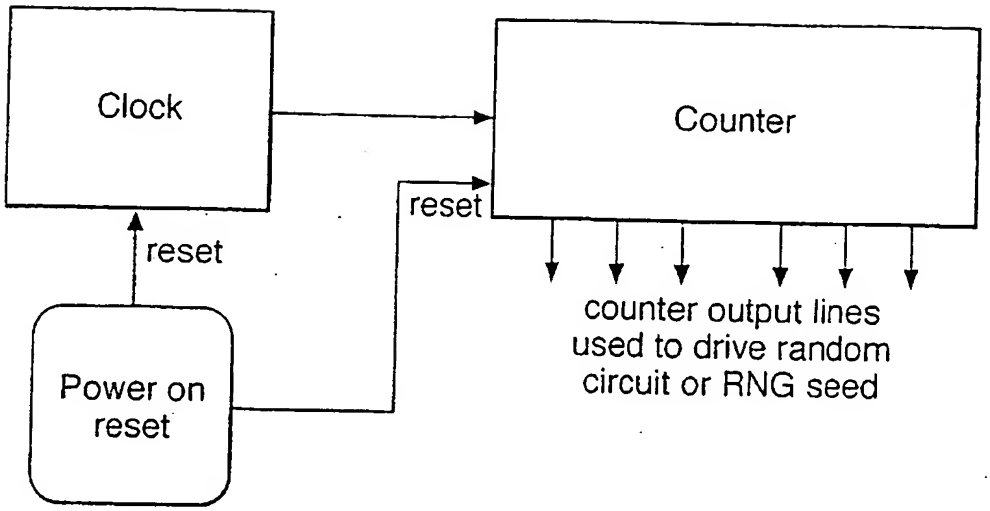
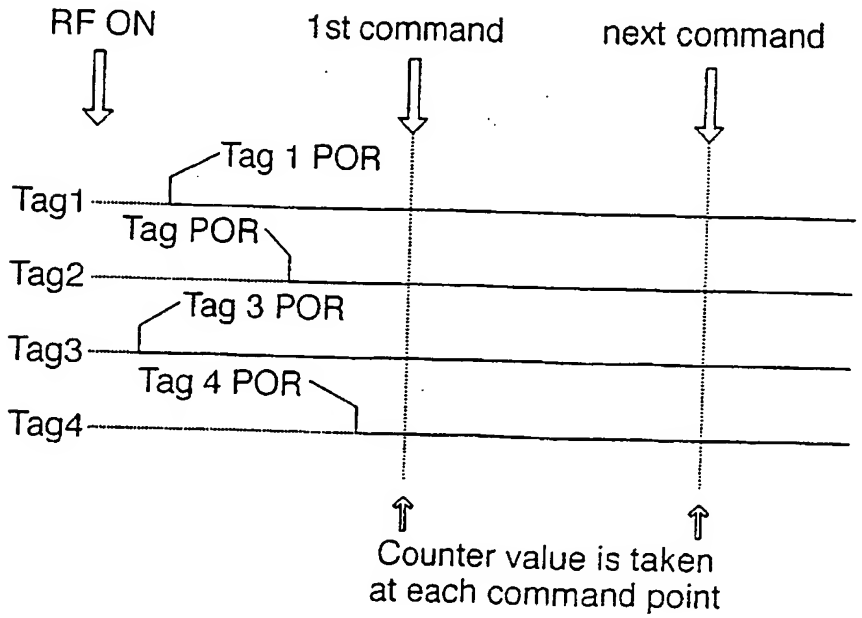

Clock
Counter
reset
reset
Power on reset
counter output lines used to drive random circuit or RNG seed

Fig.2


RF ON
1st command
next command
Tag 1 POR
Tag1
Tag POR
Tag2
Tag 3 POR
Tag3
Tag 4 POR
Tag4
Counter value is taken at each command point

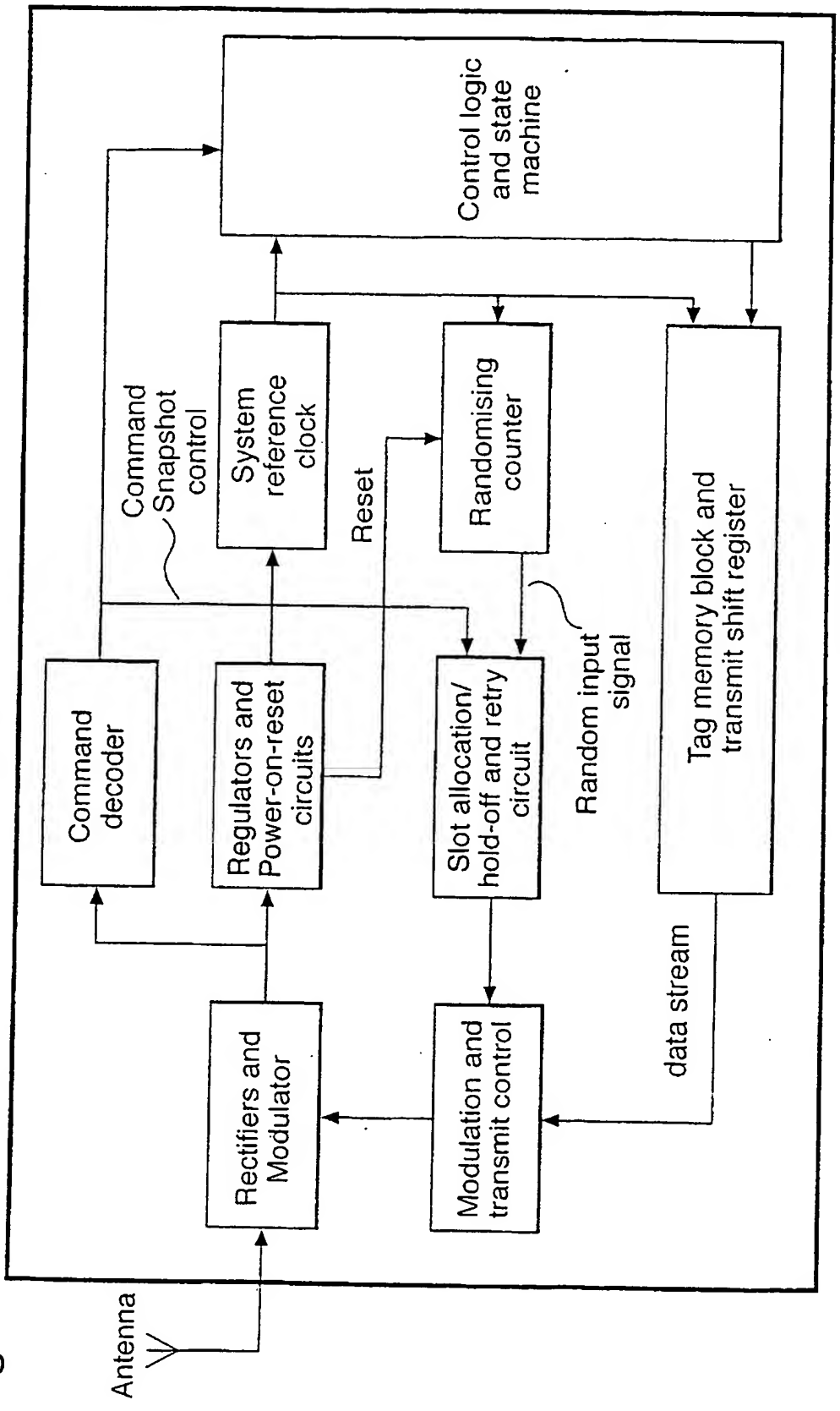

Control logic and state machine
System reference clock
Randomising counter
Tag memory block and transmit shift register
Command Snapshot control
Reset
Command decoder
Regulators and Power-on-reset circuits
Slot allocation/ hold-off and retry circuit
Random input signal
Rectifiers and Modulator
Modulation and transmit control
data stream
Antenna
RFID Chip - Block Diagram

Fig. 3

INTERNATIONAL SEARCH REPORT

Application No
PCT/GB 03/02532

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K7/00 G01S13/02 G07C9/00 G06K19/07

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K G01S G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 883 582 A (BOWERS JOHN H ET AL) 16 March 1999 (1999-03-16) abstract column 3, line 66 -column 10, line 38	1-8
A	EP 0 467 036 A (SAVI TECHN INC) 22 January 1992 (1992-01-22) cited in the application column 7, line 2 - line 20; figure 10	1-8
A	EP 1 017 005 A (INTEGRATED SENSOR SOLUTIONS) 5 July 2000 (2000-07-05) paragraph '0003!	1-8

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 September 2003	16/10/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Heusler, N

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Application No
PCT/GB 03/02532

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5883582 A	16-03-1999	AU 723246 B2	24-08-2000
		AU 6031698 A	26-08-1998
		CN 1246947 T	08-03-2000
		EP 0958561 A1	24-11-1999
		JP 2001511276 T	07-08-2001
		TW 399190 B	21-07-2000
		WO 9835327 A1	13-08-1998
EP 0467036 A	22-01-1992	AT 134044 T	15-02-1996
		DE 69116946 D1	21-03-1996
		DE 69116946 T2	20-06-1996
		DK 467036 T3	11-03-1996
		EP 0467036 A2	22-01-1992
		ES 2082885 T3	01-04-1996
		GR 3019842 T3	31-08-1996
		JP 4232488 A	20-08-1992
		US 5640151 A	17-06-1997
		US 5528232 A	18-06-1996
		US 5686902 A	11-11-1997
		US 5973613 A	26-10-1999
EP 1017005 A	05-07-2000	US 6535109 B1	18-03-2003
		EP 1017005 A2	05-07-2000
		JP 2000174658 A	23-06-2000